

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 2:20-mj-391

Information associated with songguozheng@yahoo.com that
is stored at premises owned, maintained, controlled or
operated by Oath Holdings, Inc. ("the Provider"), a company
headquartered at 701 First Ave., Sunnyvale, CA

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

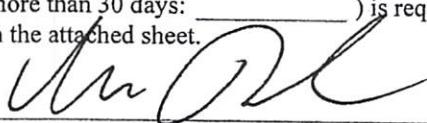
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 666	Grant Fraud
18 U.S.C. § 1001(a)(1)	Engaging in a scheme to conceal a material fact or facts

The application is based on these facts:

See Affidavit

Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Vincent Trawi - Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 5-29-20City and state: Columbus, OH

Judge's signature
Chelsey M. Vascura, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

In the matter of the search of information
associated with
songguozheng2013@yahoo.com that is
stored at premises owned, maintained,
controlled or operated by Oath Holdings,
Inc. ("the Provider"), a company
headquartered at 701 First Ave, Sunnyvale,
California

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Vincent Traul, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. As set forth in detail below, federal law enforcement is conducting an investigation into the possible violations of federal criminal laws by Songguo Zheng (ZHENG). In particular, Your Affiant submits that the facts herein establish probable cause to believe ZHENG is in violation of 18 U.S.C. § 666 (Theft or Bribery Concerning Programs Receiving Federal Funds) and 18 U.S.C. § 1001 (False Statements) (referred to as the SUBJECT OFFENSES).

2. Relevant here, I make this Affidavit in support of an application for a search warrant for information associated with songguozheng2013@yahoo.com (SUBJECT ACCOUNT) that is stored at premises controlled by (a) Oath, Inc. (formerly AOL and hereinafter "Oath"), an e-mail provider and provider of other internet services headquartered at 22000 AOL Way, Dulles, Virginia; and (b) Oath Holdings, Inc. (formerly Yahoo! And hereinafter "Oath Holdings"), an e-mail provider and provider of other internet services headquartered at 701 First Ave, Sunnyvale, California believing evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES will be found within the SUBJECT ACCOUNT. This Affidavit is made in support

of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath and Oath Holdings to disclose to the United States copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. The SUBJECT ACCOUNT is as follows:

The e-mail account songguozheng2013@yahoo.com, that is stored at premises owned, maintained, controlled or operated by Oath Holdings, Inc. ("the Provider"), a company headquartered at 701 First Ave, Sunnyvale, California.

4. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. AGENT BACKGROUND

5. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since June 2014, and I am currently assigned to the Cincinnati Division, Columbus Resident Agency, as a member of the Counterintelligence Squad. I am responsible for investigating, among other crimes, the theft or bribery concerning programs receiving federal funds. I have received both formal and informal training in the detection and investigation of said offense. As a result of my training and experience, I am familiar with the federal laws relating to the theft or bribery concerning programs receiving federal funds. I have participated in various investigations, including those with a foreign counterintelligence nexus. As a federal agent, I am authorized to investigate violations of the laws of the United States.

6. I have personally participated in the investigation described herein. I have reviewed the relevant documents and reports of witness interviews during the course of this investigation.

The statements contained in this Affidavit are based on my own observations, document reviews, and reliable information provided to me by other law enforcement officials. Because this Affidavit is being submitted for the limited purpose of establishing probable cause to search the property described below, I have not included each and every fact learned during the course of this investigation. Rather, I have set forth those facts that I believe are necessary to establish probable cause for the search warrant sought. Where actions, conversations, and statements of others are related, they are related in part, except where otherwise indicated.

7. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that violations of the SUBJECT OFFENSES have been committed by ZHENG. There is also probable cause to believe that fruits, evidence, and instrumentalities of these crimes in the form of electronic communications, as described in Attachment B, are located at the e-mail service provider, as described in Attachment A.

III. JURISDICTION

8. Pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) & (c)(1)(A), the United States may require a provider of an electronic communications service or remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to subscribers, by obtaining a warrant issued using the procedures described in Federal Rule of Criminal Procedure 41.

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States... that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

IV. APPLICABLE STATUTES AND DEFINITIONS

10. I am advised that:

a. Title 18, United States Code, Section 666(a)(1)(A) states, in relevant part:

(a) Whoever, if the circumstances described in subsection (b) of this section exists—

(1) being an agent of an organization, or of a State, local, or Indian tribal government, or any agency thereof—

(A) embezzles, steals, obtains by fraud, or otherwise without authority knowingly converts to the use of any person other than the rightful owner or intentionally misapplies, property that—(i) is valued at \$5,000 or more, and (ii) is owned by, or is under the care, custody, or control of such organization, government or agency . . . shall be fined under this title, imprisoned not more than 10 years, or both.

b. Title 18, United States Code, Section 666(b) states, in relevant part: “The circumstances referred to in subsection (a) . . . is that the organization, government, or agency receives, in any one year period, benefits in excess of \$10,000 under a Federal program involving a grant . . .”

c. The provisions of 18 U.S.C. § 666 and its subparts cover, among other crimes, the crimes of embezzlement, fraud, or conversion, so far as those crimes concern any property, regardless of whether the property itself can be traced directly as federal property—as long as the owner of the property, which is an organization, or State or local government, received \$10,000 in federal funds, and so long as the property is valued at \$5,000 or more. *See, e.g., United States v. Valentine*, 63 F.3d 459, 464 (6th Cir. 1995) (“Thus, we find that the statute does not require the government to demonstrate the federal character of stolen property. The statute addresses the relationship between the federal government and the local government from which the property was stolen, not the relationship between the federal government and the converted property.”)

11. Title 18, United States Code, Section 1001(a) provides, in relevant part, that “whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact” or “makes any materially false, fictitious, or fraudulent statement or representation” is in violation of federal law.

V. INVESTIGATION AND PROBABLE CAUSE

Overview

12. I am currently investigating ZHENG for committing grant fraud (18 U.S.C. § 666) and engaging in a scheme to conceal a material fact or facts (18 U.S.C. § 1001(a)(1)) related to more than approximately \$4,339,000 in grant funding that ZHENG and his research group(s) received from the National Institutes of Health (NIH). NIH revealed that ZHENG has received funds and serves as the Principal Investigator (PI) on two active NIH awards, R01 AR059103, with funds totaling approximately \$3,573,000, and R61 AR073049, with funds totaling approximately \$766,000. ZHENG also has one pending NIH award, R01 AR077009, for which he has not yet received funds. In addition, based upon open source information derived from ScienceNet.cn¹, accessed by NIH on 4/14/2020 (fund.sciencecn.net.cn), NIH noted ZHENG also appears to have received funding from and is listed as the Project Manager (PM) on at least three National Natural Science Foundation of China (NNSFC) grants which have overlapping timeframes with NIH grants R61 AR073049 and R01 AR059103. This overlap, which was not disclosed by ZHENG to NIH, potentially violates Title 18, United States Code, Section 666. The NNSFC grants associated with ZHENG include Numbers 30728007, 81871224, and 81671611.

¹ According to its Wikipedia page, ScienceNet.cn is a science virtual community and science blog that is supported by the Chinese Academy of Sciences (CAS) and the NNSFC with a mission of establishing a global Chinese science community.

As part of the NIH Grant applications, ZHENG made either untimely, incomplete or no disclosure of foreign components, foreign affiliation, or foreign funding, potentially violating Title 18, United States Code, Section 1001.

Background on NIH Grants and Policies

13. A component of the United States Department of Health and Human Services, NIH is a Government agency responsible for biomedical and public health research. The NIH conducts its own scientific research through an intramural research program, and also provides major biomedical research funding to non-NIH research facilities through an extramural research program. Many of the non-NIH research facilities that receive funding through NIH's extramural research program are colleges and universities, including OSU.

14. In order to receive NIH funding, non-NIH research institutions must submit a detailed application describing, among other things, the purpose and scope of the proposed research, the amount of funding requested, and how the funding will be used. Both during the application process and periodically after an award is made, the institution must also disclose to NIH all foreign collaboration and foreign sources of research support, including, but not limited to, research grants, cooperative agreements, contracts and/or institutional awards.² Additionally, NIH requires research institutions to identify and disclose to NIH significant (typically greater than \$5,000) financial conflicts of interest (COI) by investigators (that is, the person or persons responsible for the design, conduct, and reporting of research), including those related to funds

² NIH Grants Policy Statement, Section 1.2, defines "other support" as "all financial resources, whether Federal or non-Federal, commercial or institutional, available in direct support of an individual's research endeavors, including but not limited to research grants, cooperative agreements, contracts, and/or institutional awards. This includes research support from foreign governments or entities. Applicants must provide updated other support information prior to award via just-in-time and are required to identify any changes in other support in each annual progress report."

received from a foreign institution of higher education or the government of another country.³ Although it is the research institution itself that submits the grant application and all other grant-related disclosures to NIH, the individual investigator(s) must certify to the institution and NIH that the information contained in grant applications, post-award submissions, and all other grant-related filings is accurate and complete, and also acknowledge that any false, fictitious, or fraudulent statements or claims made to NIH may subject the PI to criminal, civil, and/or administrative penalties.

Background on OSU Policies

15. According to OSU, the policies applicable to faculty at OSU, which ZHENG is considered, include the Faculty Financial Conflict of Interest Policy (FCOI), the Faculty Paid External Consulting Policy (FPEC), the Faculty Conflict of Commitment Policy (FCCP) and the Faculty Compensation Policy (FCP). These policies are all available via OSU's Office of University Compliance and Integrity website.

16. According to the FCOI Policy, "a conflict of interest exists if financial interests or other opportunities for tangible personal benefit may exert a substantial and improper influence upon a faculty member or administrator's professional judgement in exercising any institutional responsibility."

17. Significant financial interest as defined by OSU's FCOI Policy includes any equity interest in a non-publicly traded entity or any financial remuneration received from the entity in the twelve months preceding the disclosure that, when aggregated, exceeds \$5,000.

³ Public Health Service (PHS) Financial Conflict of Interest Regulations, 42 CFR 50, Subpart F, require investigators to disclose to their institution all significant financial interests including those related to funds received from a foreign institution of higher education or the government of another country.

18. Your Affiant has reviewed OSU's FCOI Policy which indicates that it requires financial interest disclosures to be filed annually. In addition, according to the policy, "Updates must be made to the disclosure within thirty (30) days if the filing party acquires any new financial interests, external professional activities, or business or financial transactions that were previously unreported, or if changes occur in the circumstances of a previously reported transaction or activity."

19. OSU's FPEC Policy, dated 5/14/2012 states, "Faculty members are encouraged to engage in paid external consulting to the extent that these activities do not entail a conflict of interest as defined in the Conflict of Interest Policy." In addition, the policy states, "a faculty member must complete the Paid External Consulting Approval Form for each consulting arrangement and all paid external consulting related to one's area of expertise requires prior approval." It further states, "if a proposed consulting arrangement causes or could be perceived to cause a potential conflict of interest, the faculty member must file a Conflict of Interest Form along with the Paid External Consulting Approval Form."

20. Additionally, OSU provides a COI 'Frequently Asked Questions' section via OSU's Office of Research Compliance web page (<https://orc.osu.edu/regulations-policies/coi/faqs/>). This website, which was reviewed by Your Affiant on 5/8/2020, states, "Any external activity that could reasonably related to your institutional responsibilities must be disclosed (which includes personal activities with foreign governments, foreign academic institutions, and other foreign entities)." Further, it states, "Examples of a foreign relationship include: Participating in a Foreign Talent Recruitment Program (e.g. Thousand Talents Program, Yangtze River Scholars)..." According to OSU, the aforementioned COI language regarding Foreign Talent Recruitment Programs was employed by OSU on or around 1/2/ 2019.

21. OSU requires certain faculty to submit an annual COI Disclosure to OSU via OSU's e-COI disclosure process. The e-COI disclosure process serves as the single disclosure mechanism for three different potential types of conflicts, which includes Research-related conflicts that are reviewed by the Office of Research Compliance. In order for faculty to submit the COI Disclosures, they must visit the same Office of University Compliance and Integrity website, mentioned in paragraph 15, and log into OSU's e-COI Disclosure system. As part of the e-COI submission, the faculty member electronically completes and signs their applicable disclosure forms.

22. As it relates to the submission of grant proposals to NIH, OSU's Office of Sponsored Programs receives a completed grant proposal packet directly from the PI, via the PI's OSU e-mail. Once received via e-mail, the Office of Sponsored Programs uploads the grant proposal into NIH's portal.

Background on ZHENG

23. Your Affiant confirmed the following information through communications with OSU, a review of OSU records, as well as documentation obtained from NIH. ZHENG works as a professor and researcher at OSU in the field of Rheumatology and Immunology and has been with the university since approximately January 2019. ZHENG is the Ronald L. Whisler Chair in Rheumatology and Immunology and Professor of Internal Medicine located at the OSU Wexner Medical Center and College of Medicine. As the Whisler Chair in Rheumatology and Immunology at OSU, ZHENG is in charge of a \$2 million endowment that was established by OSU to support world-class autoimmune research and scholarship. ZHENG's expertise locates on the pathogenesis, cytokines and immune regulation of autoimmune, allergic and inflammatory disease. He is a pioneer in the field of gingiva-derived mesenchymal stem cells (GMSC) and

immunoregulation. In addition, ZHENG is an editor and editorial board member for several journals and is a member and reviewer of multi-NIH study sections. Prior to joining OSU, ZHENG was a Professor of Medicine and Director of Rheumatology Research in the Department of Medicine at Pennsylvania State University (PSU) Hershey College of Medicine from approximately 2013 – 2019. Prior to PSU, ZHENG was a post-doctoral fellow, Assistant Professor and an Associate Professor at the Keck School of Medicine, Division of Rheumatology at the University of Southern California from approximately 2000 – 2012.

24. According to NIH applications submitted by ZHENG and his associated universities, ZHENG has been awarded two separate NIH grants since on or about 11/19/2009, which included approximately eight different applications. As of the date of this affidavit, total funding awarded between the two grants totaled approximately \$4,339,000. ZHENG also applied for a third grant on 3/30/2020 which is pending NIH approval as of the date of this affidavit. As part of the NIH grant applications, ZHENG made either untimely, incomplete or no disclosure of foreign components, foreign affiliation, or foreign funding related to his affiliations with Third Affiliated Hospital at Sun Yat-Sen University (TAH) or Chinese Talent Plans⁴.

ZHENG's False Statements in NIH Grant Applications

25. On or around 4/30/2020, NIH revealed they were investigating ZHENG for possible non-compliance with NIH policies regarding disclosure of outside research support and relevant affiliations or foreign components to OSU.

26. Based upon Your Affiant's review of NIH applications, just-in-time submissions and Reporting Period Progress Reports (RPPR), opportunities for disclosure of "other support" by

⁴ The term "Chinese Talent Plans" (CTP) refers collectively to hundreds of diverse plans designed by the Chinese government to recruit, cultivate, and attract high-level scientific talent in furtherance of China's scientific development, economic prosperity, and national security.

the PI are built into the aforementioned processes. As part of the application process, ZHENG submitted an application for NIH grants R61 AR073049 and R01 AR059103 on 4/19/2019. The applications called for the disclosure of any “Ongoing Research Support.” In his grant applications, ZHENG disclosed ongoing research related to other NIH affiliated projects but did not disclose his Chinese grants, 81671611, active 1/1/2017 through 12/31/2020, and 81871224, active 1/1/2019 through 12/31/2019. Further, as part of the annual review process, ZHENG submitted a Reporting Period Progress Report (RPPR) regarding NIH grant R01 AR059103 on 4/8/2016, 3/13/17, 1/16/2019 and 1/15/2020. The RPPR, in Section D.2.c seeks information on “Changes in Other Support.” In three of the four RPPRs, ZHENG disclosed changes to ongoing research related to NIH projects, but in all four of the submissions, ZHENG did not disclose his active Chinese grants. Based on a review of the timeframes of the four RPPR submissions noted above, the active Chinese grants should have been captured. According to NIH, no RPPRs were submitted by ZHENG for grant R61 AR073049.

27. Based on information from NIH, NIH grant R61 AR073049, in the amount of approximately \$382,881, was initially awarded to ZHENG, as the PI, through PSU Hershey Medical Center, on or about 2/27/2018. The grant was subsequently submitted for a ‘Change of Grantee Organization’ to OSU by ZHENG on or about 4/19/2019 due to his institution transfer. The grant (7 R61 AR073049-03) was renewed and awarded to OSU on or about 7/30/2019, in the amount of \$307,788, and listed ZHENG as the PI. The projected start and end dates of the project were on or about 4/20/2019 and 8/31/2019, respectively. No disclosure of foreign components, foreign affiliation, or foreign funding was included with either the Change of Grantee Organizations, renewal or in the original application.

28. Additionally, NIH reports that grant R01 AR059103, in the amount of approximately \$364,500, was initially awarded to ZHENG, as the PI, through the University of Southern California (USC), on or about 6/28/2010. The grant was subsequently submitted for a 'Change of Grantee Organization' to PSU by ZHENG on or about 8/13/2013, due to his institution transfer, and was then submitted for another 'Change of Grantee Organization' by ZHENG on or about 4/19/2019 due to his institution transfer to OSU. The grant (7 R01 AR059103-10) was renewed and awarded to OSU on or about 7/29/2019, in the amount of approximately \$343,200, and listed ZHENG as the PI. The projected start and end dates of the project were on or about 7/1/2010 and 2/28/2021, respectively. Other than on one occasion, when an untimely and suspected incomplete disclosure was made via a Revision Application to grant renewal 2 R01 AR059103-07, no disclosure of foreign components, foreign affiliation, or foreign funding was included with either the Change of Grantee Organizations, renewals or in the original application. Regarding the aforementioned Revision Application, a revision was submitted on 3/3/2016 for an 'Administrative Supplement' to 2 R01 AR059103-07 that was originally submitted on 6/30/2014. Included in the revision application, which was submitted 612 days after the original renewal application, ZHENG listed in the 'Ongoing Research Support' portion of his 'Biographical Sketch' section that he was the PI for a Sun Yat-Sen University Key Project from 7/1/2014 – 6/30/2017.

29. As of the date of this Affidavit, NIH records indicate there is a grant application, R01 AR077009, with ZHENG listed as the PI that is pending review by NIH's Integrated Review Group (IRG). As part of the application, no disclosure of foreign components, foreign affiliations, or foreign funding was provided by ZHENG.

Facts Indicating ZHENG's Research Support from Foreign Governments or Entities

30. Based on open source information (<https://fund.sciencecn.net/project/440336>), it was revealed that funding from the NNSFC, via Approval Number 81671611, was awarded to Sun Yat-Sen University (SYU), with ZHENG listed as the PM. The funding awarded was “60.00 Ten Thousand yuan” and the research period was listed as 1/1/2017 through 12/31/2020. Based on my training and experience, “60.00 Ten Thousand yuan” is the equivalent to 600,000 yuan (approximately \$86,419 USD as of 1/1/2017). Based on the aforementioned information, Approval Number 81671611 included dates that overlapped with both NIH Awards R61 AR073049 and R01 AR059103.

31. Based on open source information (<https://fund.sciencecn.net/project/492772>), it was revealed that funding from the NNSFC was awarded to SYU, with ZHENG listed as the PM via Approval Number 81871224. The funding awarded was “57.00 Ten Thousand yuan” and the research period was listed as 1/1/2019 through 12/31/2019. Based on my training and experience, “57.00 Ten Thousand yuan” is the equivalent to 570,000 yuan (approximately \$82,866 USD as of 1/1/2019). Based on the aforementioned information, Approval Number 81871224 included dates that overlapped with both NIH Awards R61 AR073049 and R01 AR059103.

32. Based on open source information (<https://fund.sciencecn.net/project/118204>), it was revealed that funding from the NNSFC was awarded to SYU, with ZHENG listed as the PM via Approval Number 30728007. The funding awarded was “40.00 Ten Thousand yuan” and the research period was listed as 1/1/2008 through 12/31/2010. Based on my training and experience, “40.00 Ten Thousand yuan” is the equivalent to 400,000 yuan. Based on the aforementioned information, Approval Number 30728007 included dates that overlapped with NIH Award R01 AR059103.

ZHENG's Hundred and Thousand Talents Plan Participation

33. Open source research of TAH's Professor Home Page, viewed by Your Affiant on 5/8/2020 (www.zssy.com.cn:8080/professor/intro?id=258), revealed ZHENG's professional titles also include or have included, "Professor at Sun Yat-Sen University", located in Guangzhou, Guangdong Province, China; "Director, Clinical Immunology Center, Third Affiliated Hospital at Sun Yat-Sen University"; "Expert of Thousand Talents Program"; and, "Full Professor (with tenure) and Director, Autoimmunity Center, Penn State University Hershey Medical College". Per ZHENG's OSU Biography Page, dated 7/31/2019, no affiliations were listed related to the aforementioned titles.

34. In addition to his work at OSU, ZHENG has conducted work with and for various institutions in China. According to the aforementioned Professor Home Page, which included a bio about ZHENG, located on a website run by the TAH, (www.zssy.com.cn:8080/professor/intro?id=258), viewed by Your Affiant on 5/8/2020, ZHENG is listed as being a Professor with the Department of Clinical Immunology Center, as well as the Director of the Clinical Immunology Center, and that his research focuses on the development and function of regulatory T (Treg) cells in autoimmune diseases, GVHD and organ transplantation.

35. Open source research conducted on 8/19/2019 identified an article dated 3/9/2014, titled, "The Third Affiliated Hospital of Sun Yat-Sen University, on the open recruitment of leading talent, Professor Songguo Zheng, research assistant" wherein ZHENG is identified as "a leading talent of the 'Hundred Talents Program' (HTP) of SYU" and that ZHENG "publicly recruited a research assistant at home and abroad for the work of scientific research laboratories and international exchanges." Further, an article dated 9/13/2018, titled, "Songguo Zheng – Hanshi Xu joint group found that rheumatoid arthritis fibroblast-like synoviocytes invade secrets"

identified ZHENG as an “Expert of the National Thousand Talents Program of the China Central Organization Department”.

36. In an article viewed by Your Affiant on 5/6/2020, via SYU’s Office of Scientific Research and Development website (<http://research.sysu.edu.cn/node/1778>), ZHENG was selected as one of six leaders included in the sixth batch of the Pearl River Talent Program (PRTP). It is believed the sixth batch of the PRTP was selected in or around May 2017. In the announcement, it was noted ZHENG’s research team name was “Clinical Immunology Precision Diagnosis and Treatment Translational Medicine Innovation Team”, the research area was listed as “Biotechnology and New Medicine” and the employer was listed as the “Third Affiliated Hospital”. The PRTP was launched in 2009 and supports innovative talents and teams in the Guangdong Province, China.

37. Based on open source research, conducted by Your Affiant on 5/8/2020, of SYU’s Office of Scientific Research and Development – Announcement web page (<http://research.sysu.edu.cn/notice>) it appeared the announcement publication of article 1778 (noted above) had been removed, although the webpage (<http://research.sysu.edu.cn/node/1778>), was still active. On 5/8/2020, Your Affiant reviewed the Announcement web page (<http://research.sysu.edu.cn/notice?page=51>) and identified article 1777 (<http://research.sysu.edu.cn/node/1777>), which appears to be the article published immediately before article 1778. Article 1777 is noted as being written on 5/11/2017 and appears to have been published on 5/12/2017. Further, Your Affiant identified article 1779 (<http://research.sysu.edu.cn/node/1779>), which appears to be the article published immediately after article 1778. Article 1779 was noted as being written on 5/8/2017 and appears to have been published on 5/12/2017. Therefore, Your Affiant has reason to believe article 1778 was published

on or around 5/12/2017 indicating ZHENG was selected to the sixth batch of the PRTP in or around May 2017.

38. In an article published on or around 11/24/2017, via a medical resource website (www.kanyixue.com), titled, “Guangdong Zhongshan Third Hospital of Guangzhou Open Recruitment Clinical Immunology Center Professor Zheng Songguo's research team”, it appeared ZHENG was seeking to recruit six research assistants (four masters and two undergraduates) to his Clinical Immunology Precision Diagnosis and Treatment Translational Medicine Innovation Team to conduct research at TAH and its branches.

39. Based on my training, experience, and involvement in investigations related to the PRC Government's talent-recruitment activities, review of open-source reporting and other materials, and conversations with other law enforcement officers, I have learned the following:

- a. The Chinese Communist Party (CCP) is the ruling party of the People's Republic of China (PRC). The Central Committee of the Communist Party of China is a political body that comprises the top leaders of the CCP and the State Council is the chief administrative authority of the PRC.
- b. In or around 2008, the PRC Government launched a talent-recruitment program officially known as the “Recruitment Program of Global Experts,” commonly referred to as the “Thousand Talents Plan.” The Thousand Talents Plan (TTP) aims to recruit overseas scientists, engineers, and other experts to work for businesses, research institutes, and government agencies in China, with the goal of utilizing these experts to further the PRC Government's strategic national development goals.

- c. TTP recruits typically sign contracts that detail the specific research the recruit will perform or the business the recruit will develop in China. That contractual obligation often resembles or even replicates the work the recruit performs or performed for his or her U.S.-based or other overseas employer, thereby leveraging the recruit's knowledge and access to intellectual property obtained from U.S. and foreign businesses, government laboratories, and research institutions.
- d. According to China University of Mining and Technology's website from 1/1/2017, CTPs include four different types – Full Time/Business, Young Talents, Non-Chinese and Part Time. The time frame requirements vary between the four types but require a minimum of three to five years of service.
- e. On or about 5/19/15, the State Council issued the PRC's first ten year action plan "Made in China 2025" which is a state-led program to further technological and economic growth in China. As part of the plan, the PRC funds and directs the acquisition of foreign technology and intellectual property. Included as one of the ten key sectors of the "Made in China 2025" plan was bio-medicine.

ZHENG's Misrepresentations and Omissions Regarding His Chinese Grants and Involvement with the TAH and the PRTP Related to OSU's COI Policies and NIH Grants

40. ZHENG has engaged in conduct that, based on training and experience, Your Affiant respectfully submits supports a probable cause determination that ZHENG has violated federal law that prohibits making materially false misrepresentations to law enforcement in violation of 18 U.S.C. §§ 666 and 1001 — in particular with respect to his involvement with the TAH and the PRTP. To this end, Your Affiant respectfully offers the following:

41. ZHENG is subject to conflicts of interest disclosures given his work at OSU, and because of his grant application(s) to, and receipt of grant money from, NIH.

42. OSU has provided the following information from their official records, policies and procedures:

43. ZHENG has been a professor at OSU since in or around January 2019. With respect to the time periods relevant to this Affidavit, ZHENG made his COI disclosures for 2018 and 2019 to OSU on or around 2/12/2019 and 4/16/2019, respectively, via the e-COI Disclosure portal. At that time, OSU's FCOI Policy, which was edited on 5/1/2018, and which was the FCOI Policy in place at the time of ZHENG's grant applications, required disclosure to OSU of external financial interests that could be viewed as a conflict of interest between the professor and the University. In both COI disclosures noted above, ZHENG completed disclosures related to OSU's Office of Research Compliance, their Office of University Compliance and Integrity and the OSU Wexner Medical Center and self-approved that he had no significant financial interest that is related to institutional responsibilities. Additionally, as noted in paragraph 19 above, ZHENG never filed the required Paid External Consulting Approval Form and/or Conflict of Interest Form with OSU regarding his CTP affiliation.

44. Regarding NIH:

a. Your Affiant reviewed 42 CFR 50, Subpart F, "Responsibility of Applicants for Promoting Objectivity in Research for which PHS Funding is Sought" (FCOI Regulation) Section 50.604 which mandates that NIH-funded researchers disclose significant financial interests to their institution (in ZHENG's case, OSU), either at the time of application for PHS-funded research, annually, or within 30 days of discovering or acquiring a new significant financial interest. Based upon Your Affiant's training and experiences, the institution is the conduit to disclosing this information to NIH.

b. A review of NIH records reveals that on or about 4/19/2019, ZHENG submitted electronically for a Change of Grantee Organization regarding an NIH federal grant in the United States utilizing the NIH's standard form to do so: SF 424, Application for Federal Assistance. The proposed project dates associated with ZHENG's application were 4/20/2019 through 8/31/2019. The amount of funding ZHENG requested for this application was \$307,788 for "Mesenchymal Stem Cells Derived from Human Gingiva (GMSC) Inhibit Bone Erosion in Autoimmune Arthritis." Through this application, ZHENG was awarded a grant from the NIH, specifically NIH grant Number 7 R61 AR073049-03.

c. Also, on or about 4/19/2019, ZHENG submitted electronically for a Change of Grantee Organization regarding an NIH federal grant in the United States utilizing the NIH's standard form to do so: SF 424, Application for Federal Assistance. The proposed project dates associated with ZHENG's application were 4/20/2019 through 1/31/2021. The amount of funding ZHENG requested for this application was \$686,400 for "Therapeutic immunoregulation mediated by TGF-beta-induced iTregs in autoimmune arthritis." Through this application, ZHENG was awarded a grant from the NIH, specifically NIH grant Number 7 R01 AR059103-10.

d. Further, NIH records indicate that on or about 3/30/2020, ZHENG submitted electronically for an NIH federal grant in the United States utilizing the NIH's standard form to do so: SF 424, Application for Federal Assistance. The proposed project dates associated with ZHENG's application were 12/1/2020 through 11/30/2025. The amount of funding ZHENG requested for this application was \$1,950,000 for "Immune regulation and therapy in rheumatoid arthritis." As of the date of this affidavit, ZHENG's application was still pending review.

e. As a standard part of the SF 424, Application for Federal Assistance, OSU's Authorized Representative, based upon information received from ZHENG, would have been

required to affirm the following: "By signing this application, I certify (1) to the statements contained in the list of certifications* and (2) that the statements herein are true, complete and accurate to the best of my knowledge. I also provide the required assurances* and agree to comply with any resulting terms if I accept an award. I am aware that any false, fictitious or fraudulent statements or claims may subject me to criminal, civil, or administrative penalties." (Your Affiant notes that, on the SF 424, the above-cited language is followed by a citation to "U.S. Code, Title 18, Section 1001").

45. With the above information as background, Your Affiant, based upon the following and upon the information noted in this Affidavit, submits that there is probable cause to believe that ZHENG has previously violated 18 U.S.C. § 1001. For example:

a. As explained in this Affidavit, ZHENG was listed as a leading talent of the HTP in 2014 and as a TTP participant via the PRTP at TAH in 2017. ZHENG likely would have begun his TTP work sometime in 2017, based upon the recruitment article seeking research assistants to join ZHENG's team at TAH and its branches that was published on or around 11/24/2017. His TTP work likely continued into 2020 or is still ongoing based upon the minimum three to five year commitment per the China University of Mining and Technology's website from 1/1/2017.

b. On or about 4/19/2019, ZHENG submitted a revision application regarding grant 7 R61 AR073049-03 for Federal Assistance from NIH with proposed project dates of 4/20/2019 through 8/31/2019, and projected funding of \$307,788. Your Affiant is aware that, just as for an initial NIH application, NIH revision applications require NIH-funded researchers to disclose outside financial interests to their employing entity.

c. ZHENG's renewal NIH application was granted on or around 7/30/2019.

d. On or about 4/19/2019, ZHENG submitted another revision application regarding grant 7 R01 AR059103-10 for Federal Assistance from NIH with proposed project dates of 4/20/2019 through 1/31/2021, and projected funding of \$686,400. Your Affiant is aware that, just as for an initial NIH application, NIH revision applications require NIH-funded researchers to disclose outside financial interests to their employing entity.

e. ZHENG's renewal NIH application was granted on or around 7/29/2019.

f. On or about 3/3/2020, ZHENG applied electronically for grant R01 AR077009-01A1 for Federal Assistance from NIH with proposed project dates of 12/1/2020 through 11/30/2025, and projected funding of \$1,950,000. Your Affiant is aware that, just as for renewal or revision NIH applications, a first NIH application requires NIH-funded researchers to disclose outside financial interests to their employing entity.

g. ZHENG's NIH application, as of the date of the affidavit, is pending review.

h. At the time of submitting the new and revision applications, ZHENG had not disclosed his employment as a TTP member to OSU, meaning that OSU and ZHENG both failed to make the required disclosure to NIH of this issue.

i. ZHENG did not disclose his TAH or TTP affiliation to OSU in a timely or complete manner. This non-disclosure is material because had the information been disclosed to OSU, OSU would have been aware of the conflict of interest and would not have submitted any applications to NIH via their portal.

j. ZHENG was aware that making false statements or misstatements was against the law because having completed several SF 424s for NIH grants, as documented above, ZHENG would have been aware of the Section 17 of the form which states, "...I am aware that any false,

fictitious or fraudulent statements or claims may subject me to criminal, civil, or administrative penalties.”

There is probable cause to believe evidence of the SUBJECT OFFENSES will be found in the SUBJECT ACCOUNT.

46. There is probable cause to believe that evidence of the SUBJECT OFFENSES will be found in the SUBJECT ACCOUNT because ZHENG provided the SUBJECT ACCOUNT to OSU upon gaining employment with them in approximately January 2019 to utilize as his backup e-mail address for communications. Further, OSU reported in or around May 2020, after ZHENG was alerted by OSU to the letter they received from NIH regarding NIH’s investigation, and OSU restricted ZHENG’s access to his OSU email accounts, that ZHENG contacted OSU utilizing the SUBJECT ACCOUNT. Further, based on an interview conducted by a Federal agent on or about 5/23/2020 of YouQiu Xue, one of ZHENG’s research assistants at OSU, and subsequent documents provided to the agent during that interview by XUE, the SUBJECT ACCOUNT was provided as a method of contact for ZHENG on a Chinese grant application for NNSFC grant 81671611 from approximately 2015.

VI. BACKGROUND INFORMATION REGARDING PROVIDER SERVICES

47. PROVIDER is the provider of the internet-based account(s) identified by songguozheng2013@yahoo.com.

48. PROVIDER provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. PROVIDER accounts are typically identified by a single username, which serves as the subscriber’s default e-mail address, but which can also function as a subscriber’s username for other PROVIDER services, such as instant messages and remote photo or file storage.

49. Based on my training and experience, I know that PROVIDER allows subscribers to obtain accounts by registering on PROVIDER's website. During the registration process, PROVIDER asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases a means of payment. PROVIDER typically does not verify subscriber names.

50. Once a subscriber has registered an account, PROVIDER provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. PROVIDER subscribers can also use that same username or account in connection with other services provided by PROVIDER.⁵

51. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a PROVIDER account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on PROVIDER's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on PROVIDER's servers for a certain period of time.

52. Thus, a subscriber's PROVIDER account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing. Depending on user settings, user-generated content derived from many of these services is normally stored on PROVIDER's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the

⁵ Here, Provider's other services include e-mail, contact list, chat, and other services as noted generically above. It provides the branded services Yahoo! groups (a listserve and bulletin board service, which users can opt into), Yahoo! Messenger (an instant messaging service, which users can opt into), and Flickr (a photo storage and sharing service, which users can opt into). Yahoo does not currently provide a standalone notes or document storage service, but its smartphone application has designated "notes" and "documents" functions that operate through Yahoo's email storage.

subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on PROVIDER's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within such computer files and other information created or stored by the PROVIDER subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

53. Based on my training and experience, I know that providers such as PROVIDER also collect and maintain information about their subscribers, including information about their use of PROVIDER services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as PROVIDER also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

54. Based on my training and experience, I know that providers such as PROVIDER also collect information relating to the devices used to access a subscriber's account – such as

laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or “hardware,” some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by PROVIDER in order to track what devices are using PROVIDER’s accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier (“GUID”), device serial number, mobile network information, telephone number, Media Access Control (“MAC”) address, and International Mobile Equipment Identity (“IMEI”). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the PROVIDER account.

55. PROVIDER also allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber’s PROVIDER account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application (such as PROVIDER) to locate the device on which the application is installed. After the applicable push notification service (e.g., Apple Push Notifications (APN) or Google Cloud Messaging) sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push

Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of PROVIDER are likely to contain useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's PROVIDER account via the mobile application.

56. Based on my training and experience, I know that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

57. Based on my training and experience, I know that PROVIDER maintains records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group

of persons, used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

58. Based on my training and experience, I know that subscribers can communicate directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

59. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for PROVIDER subscribers), as well as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide PROVIDER with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

60. As explained above, information stored in connection with an Provider account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element

or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an Provider account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant of a residence. For example, e-mail communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at the relevant time. Further, information maintained by the Provider can show how and when the account was accessed or used. For example, as described below, Providers typically log the IP addresses from which users access the e-mail account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Provider account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Stored electronic data might also provide relevant insight into the e-mail account owner’s state of mind as it relates to the offense under investigation. For example, information in the Provider account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

61. Based on my training and experience, I know that evidence of who controlled, used, and/or created a PROVIDER account may be found within the user-generated content created or stored by the PROVIDER subscriber. This type of evidence includes, for example, personal correspondence, personal photographs, purchase receipts, contact information, travel itineraries,

and other content that can be uniquely connected to a specific, identifiable person or group. In addition, based on my training and experience, I know that this type of user-generated content can provide crucial identification evidence, whether or not it was generated close in time to the offenses under investigation. This is true for at least two reasons. First, people that commit crimes involving electronic accounts (e.g., e-mail accounts) typically try to hide their identities, and many people are more disciplined in that regard right before (and right after) committing a particular crime. Second, earlier-generated content may be quite valuable, because criminals typically improve their tradecraft over time. That is to say, criminals typically learn how to better separate their personal activity from their criminal activity, and they typically become more disciplined about maintaining that separation, as they become more experienced. Finally, because e-mail accounts and similar PROVIDER accounts do not typically change hands on a frequent basis, identification evidence from one period can still be relevant to establishing the identity of the account user during a different, and even far removed, period of time.

VII. CONCLUSION

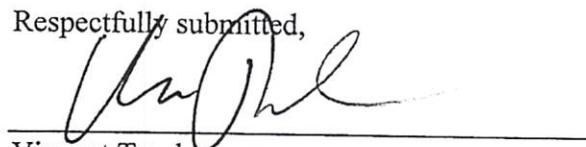
62. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on the Provider, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

VIII. REQUEST FOR SEALING

63. I further request that the Court order that all papers in support of this Application, including the Affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because

their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, tamper with or destroy evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Vincent Traul
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on May 29, 2020.



Honorable
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the Oath Holdings, Inc. account identified by the e-mail address songguozheng2013@yahoo.com and which is stored at premises owned, maintained, controlled, or operated by Oath Holdings Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Oath Holdings Inc. (the "Provider") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the United States for each account or identifier listed in Attachment A. Such information should include the below-described content of the Subject Account for the time period from account inception to the present:

1. The contents of all e-mails, opened or unopened, associated with the Subject Account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
2. Any deleted e-mails, including any information described in subparagraph "1." above;
3. All records or other information regarding the identification of the Subject Account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
4. All available IP history related to the Subject Account;
5. The types of service utilized;
6. All records or other information stored by an individual using the Provider account, including address books, contact and buddy lists, calendar data,

pictures, videos and files. In addition, please provide the photos and videos in their original file format, including EXIF information;

7. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;
8. All Provider chat archives stored on servers controlled by the Provider;
9. All location history data, search history and search queries issued;
10. A list of user accounts linked to the account by SMS, recovery e-mail, secondary email, cookie or device; and
11. All privacy settings and other account settings.

II. Information to be seized by the United States

All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages, that constitutes evidence of a crime, contraband, fruits of crime, or other items illegally possessed, or property designed for use, intended for use, or used in committing violations of 18 U.S.C. § 666 (Theft or Bribery Concerning Programs Receiving Federal Funds) and 18 U.S.C. § 1001 (False Statements), including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

1. Credit card and other financial information including but not limited to bills and payment records;
2. The identity of the person(s) who created or used the Subject Account, including records that help reveal the whereabouts of such person(s);
3. Evidence indicating how and when the e-mail account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the e-mail account owner;
4. Evidence indicating the e-mail account owner's state of mind as it relates to the crime under investigation;

5. Passwords and encryption keys, and other access information that may be necessary to access the account(s) or identifier(s) listed in Attachment B and other associated accounts;
6. All records and documents pertaining to business or LLC registration records;
7. The identity of the person(s) who communicated with the user ID about matters relating to bio-technology/bio-medicine and/or any Chinese Talent Plan.